L’attività di audit e di IT audit nelle imprese e nei gruppi assicurativi

Torino, 24 marzo 2011

Il quadro normativo di riferimento

L'evoluzione del quadro normativo di riferimento

1998

D.Lgs.58/98 Draghi

Ha introdotto in Italia i principi della "Corporate Governance" ponendo enfasi sulla rilevanza del sistema di controllo interno e sul ruolo dei soggetti che devono assicurare e vigilare sulla sua adeguatezza

Circolare n. 366 Isvap

Prescrive un nucleo minimo di indicazioni di portata generale volte a favorire la realizzazione di un adeguato sistema dei controlli interni

2000

Codice di autodisciplina della Borsa (Preda)

Suggerisce l'istituzione di un Comitato per il Controllo Interno, composto da un numero adeguato di amministratori non esecutivi, con il compito di analizzare le problematiche ed istruire le pratiche rilevanti per il controllo delle attività aziendali

D.Lgs.231/01

Ha introdotto la responsabilità amministrativa degli enti e la figura dell'Organismo di Vigilanza quale soggetto deputato al controllo sull'applicazione del Modello di Organizzazione, Gestione e Controllo

Riforma del Diritto Societario

Modifica le norme sul Collegio Sindacale allineandosi alla disciplina del TUF e pone l'accento sui requisiti soggettivi degli organi di controllo e sull'attività di vigilanza sui principi di corretta amministrazione e sul SCI

2005

Legge sul Risparmio

Interviene direttamente sulla "governance aziendale" introducendo la figura del "Dirigente preposto alla redazione dei documenti finanziari" con responsabilità, tra l'altro, sulla veridicità dei documenti pubblicati, sulla redazione di apposite procedure e sull'applicazione delle stesse.

SISTEMA DI CONTROLLO INTERNO

L'ente di controllo in ambito assicurativo

ISVAP

L'ISVAP - Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo - è un ente dotato di personalità giuridica di diritto pubblico ed è stato istituito con legge 12 agosto 1982, n. 576.

OBIETTIVI

L'esercizio della vigilanza da parte dell'ISVAP ha per scopo la **sana e prudente gestione** delle imprese di assicurazione e di riassicurazione e la **trasparenza e la correttezza dei comportamenti** delle imprese, degli intermediari e degli altri operatori del settore assicurativo, avendo riguardo alla stabilità, all'efficienza, alla competitività ed al buon funzionamento del sistema assicurativo, alla tutela degli assicurati e degli altri aventi diritto a prestazioni assicurative, all'informazione ed alla protezione dei consumatori.

L'ente di controllo nelle società quotate

CONSOB
COMMISSIONE NAZIONALE PER LE SOCIETA' E LA BORSA

La Commissione Nazionale per le Società e la Borsa (Consob), istituita con la legge n. 216 del 7 giugno 1974, è un'autorità amministrativa indipendente, dotata di personalità giuridica e piena autonomia con la legge 281 del 1985.

OBIETTIVI

L'attività della Consob ha come obiettivi la **tutela degli investitori** e l'**efficienza**, la **trasparenza** e lo **sviluppo** del mercato mobiliare. Il controllo sui prodotti finanziari, ivi inclusi i **prodotti finanziari emessi da imprese di assicurazione** (unit linked, index linked e capitalizzazioni), si realizza assicurando ai risparmiatori tutte le informazioni necessarie per effettuare e gestire i propri investimenti in modo consapevole.

Il sistema di controllo interno ed i suoi attori

Definizione del sistema dei controlli interni

DEFINIZIONE DEL SISTEMA DEI CONTROLLI INTERNI

(Regolamento ISVAP n. 20 del 26 marzo 2008)

Il sistema dei controlli interni è costituito dall'insieme delle **regole**, delle **procedure** e delle **strutture organizzative** volte ad assicurare il corretto funzionamento ed il buon andamento dell'impresa e a garantire, con un ragionevole margine di sicurezza:

a) l'efficienza e l'efficacia dei processi aziendali;

b) l'adeguato controllo dei rischi;

c) l'attendibilità e l'integrità delle informazioni contabili e gestionali;

d) la salvaguardia del patrimonio;

e) la conformità dell'attività dell'impresa alla normativa vigente, alle direttive e alle procedure aziendali.

Definizione del sistema dei controlli interni

DEFINIZIONE DEL SISTEMA DI CONTROLLO INTERNO

(Codice di Autodisciplina delle Società Quotate – Ed. 2006)

Il sistema di controllo interno è l'insieme delle **regole**, delle **procedure** e delle **strutture organizzative** volte a consentire, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi prefissati.

L'evoluzione normativa in ambito assicurativo

ISVAP

NORMAZIONE SUL SISTEMA DEI CONTROLLI INTERNI

Circolare ISVAP n. 366/D del 1999

Prescrizione di un nucleo minimo di indicazioni di portata generale volte a favorire la realizzazione di un adeguato sistema dei controlli interni.

Costituzione della **funzione di revisione interna**, con caratteristiche di autonomia e indipendenza.

Circolare ISVAP n. 577/D del 2005

Nuove indicazioni volte a favorire la realizzazione di adeguati sistemi di controllo interno e di gestione dei rischi, tenuto conto dell'evoluzione del quadro regolamentare europeo verso un nuovo regime di solvibilità maggiormente orientato ad un approccio per "rischi".

Costituzione della **funzione di Risk Management**, nel rispetto del principio di separatezza tra funzioni operative e di controllo.

Regolamento ISVAP n. 20 del 2008

Rafforzamento dei requisiti qualitativi di gestione, che unitamente ai requisiti prudenziali di tipo quantitativo, rappresentano i presidi a salvaguardia della stabilità delle imprese e dei gruppi assicurativi.

Costituzione della **funzione di Compliance**, nel rispetto della separatezza con le funzioni operative e le altre funzioni di controllo.

ISVAP – Circolari e Regolamenti: disposizioni inerenti l'I.T.

CIRCOLARE ISVAP 366/D DEL 1999

- le principali disposizioni inerenti i sistemi informativi -

ATTIVITA' DI REVISIONE INTERNA

Nell'esercizio della propria attività, la revisione interna avrà, tra l'altro, la funzione di verificare:

a) i processi gestionali e le procedure organizzative;

b) la regolarità e la funzionalità dei flussi informativi tra settori aziendali;

c) **l'adeguatezza dei sistemi informativi e la loro affidabilità affinché non sia inficiata la qualità delle informazioni sulle quali il vertice aziendale basa le proprie decisioni;**

d) la rispondenza dei processi amministrativo contabili a criteri di correttezza e di regolare tenuta della contabilità.

Affinché il sistema informatico utilizzato dall'azienda funzioni correttamente sarà necessario verificare, in modo particolare, che:

- **non vengano apportate modifiche non autorizzate al sistema**;
- esistano **procedure formalizzate per l'approvazione dell'acquisizione sia dell'hardware che del software** in modo che i nuovi applicativi introdotti in azienda siano conformi ai requisiti stabiliti dal vertice aziendale;
- vi sia **continuità operativa**;
- i dati, le informazioni e i beni informatici gestiti dalla compagnia siano salvaguardati e quindi esistano **sistemi di sicurezza contro la perdita o l'alterazione di dati o programmi**.

ISVAP – Circolari e Regolamenti: disposizioni inerenti l'I.T.

CIRCOLARE ISVAP 577/D DEL 2005
REGOLAMENTO ISVAP 20 DEL 2008
- le principali disposizioni inerenti i sistemi informativi -

FLUSSI INFORMATIVI E CANALI DI COMUNICAZIONE

(…)

Il sistema dei controlli interni deve garantire che le **informazioni abbiano le seguenti caratteristiche**:

a) **accuratezza**: le informazioni devono essere verificate al momento della ricezione e anteriormente rispetto al loro uso;

b) **completezza**: le informazioni devono coprire tutti gli aspetti rilevanti dell'impresa in termini di quantità e qualità, inclusi gli indicatori che possono avere conseguenze dirette o indirette sulla pianificazione strategica dell'attività;

c) **tempestività**: le informazioni devono essere puntualmente disponibili, in modo da favorire processi decisionali efficaci e consentire all'impresa di prevedere e reagire con prontezza agli eventi futuri;

d) **coerenza**: le informazioni devono essere registrate secondo metodologie che le rendano confrontabili;

e) **trasparenza**: le informazioni devono essere presentate in maniera facile da interpretare, garantendo la chiarezza delle componenti essenziali;

f) **pertinenza**: le informazioni utilizzate devono essere in relazione diretta con la finalità per cui vengono richieste ed essere continuamente rivedute e ampliate per garantirne la rispondenza alle necessità dell'impresa.

(…)

ISVAP – Circolari e Regolamenti: disposizioni inerenti l'I.T.

SISTEMI INFORMATICI

I sistemi informatici devono essere appropriati rispetto alle dimensioni e all'attività dell'impresa e devono fornire informazioni, sia all'interno che all'esterno, rispondenti alle caratteristiche di cui al paragrafo FLUSSI INFORMATIVI E CANALI DI COMUNICAZIONE.

A tal fine:

a) **il Consiglio di amministrazione approva un piano strategico sulla tecnologia della informazione e comunicazione (ICT),** volto ad assicurare l'esistenza e il mantenimento di una architettura complessiva dei sistemi altamente integrata sia dal punto di vista applicativo che tecnologico e adeguata ai bisogni dell'impresa;

b) **gli ambienti di sviluppo e di produzione sono separati**. Gli accessi ai diversi ambienti sono regolamentati e controllati attraverso procedure disegnate tenendo conto dell'esigenza di limitare i rischi di frode derivanti da intrusioni esterne o da infedeltà del personale. A tal fine le procedure garantiscono la sicurezza logica dei dati trattati, restringendo, in particolare per l'ambiente di produzione, l'accesso ai dati stessi a soggetti autorizzati e prevedono che tutte le violazioni vengano evidenziate; le procedure sono soggette a verifiche da parte della funzione di revisione interna;

c) **le procedure per l'approvazione e l'acquisizione dell'hardware e del software, nonché per la cessione all'esterno di determinati servizi, sono formalizzate;**

d) sono adottate procedure che assicurino la sicurezza fisica dell'hardware, del software e delle banche dati, anche attraverso **procedure di disaster recovery e back up;**

e) al fine di **garantire la continuità dei processi dell'organizzazione**, sono adottate e documentate procedure e standard operativi orientati alla individuazione e gestione degli eventi che possono pregiudicare la continuità del business, quali, in via esemplificativa, eventi imprevisti, black-out, incendi, allagamenti, malfunzionamenti dei componenti hardware e software, errori operativi da parte del personale incaricato della gestione dei sistemi o da parte degli utenti, introduzione involontaria di componenti dannosi per il sistema informativo e di rete, atti dolosi miranti a ridurre la disponibilità delle informazioni.

ISVAP – Circolari e Regolamenti: disposizioni inerenti l'I.T.

In caso di fusioni, acquisizioni di portafoglio o operazioni simili, viene predisposto un piano di integrazione dei sistemi informatici nel quale sono specificati:

a) ambiti, funzioni, procedure, applicazioni e basi dati interessate dal processo di integrazione;
b) la tempistica associata a ciascuna fase dell'integrazione con particolare riguardo alla migrazione delle basi dati e alle date a partire dalle quali l'integrazione dei portafogli (premi, sinistri etc.) sarà completata;
c) le unità e i presidi organizzativi ai quali sono affidati i controlli ed il monitoraggio dell'intero processo di integrazione.

REVISIONE INTERNA

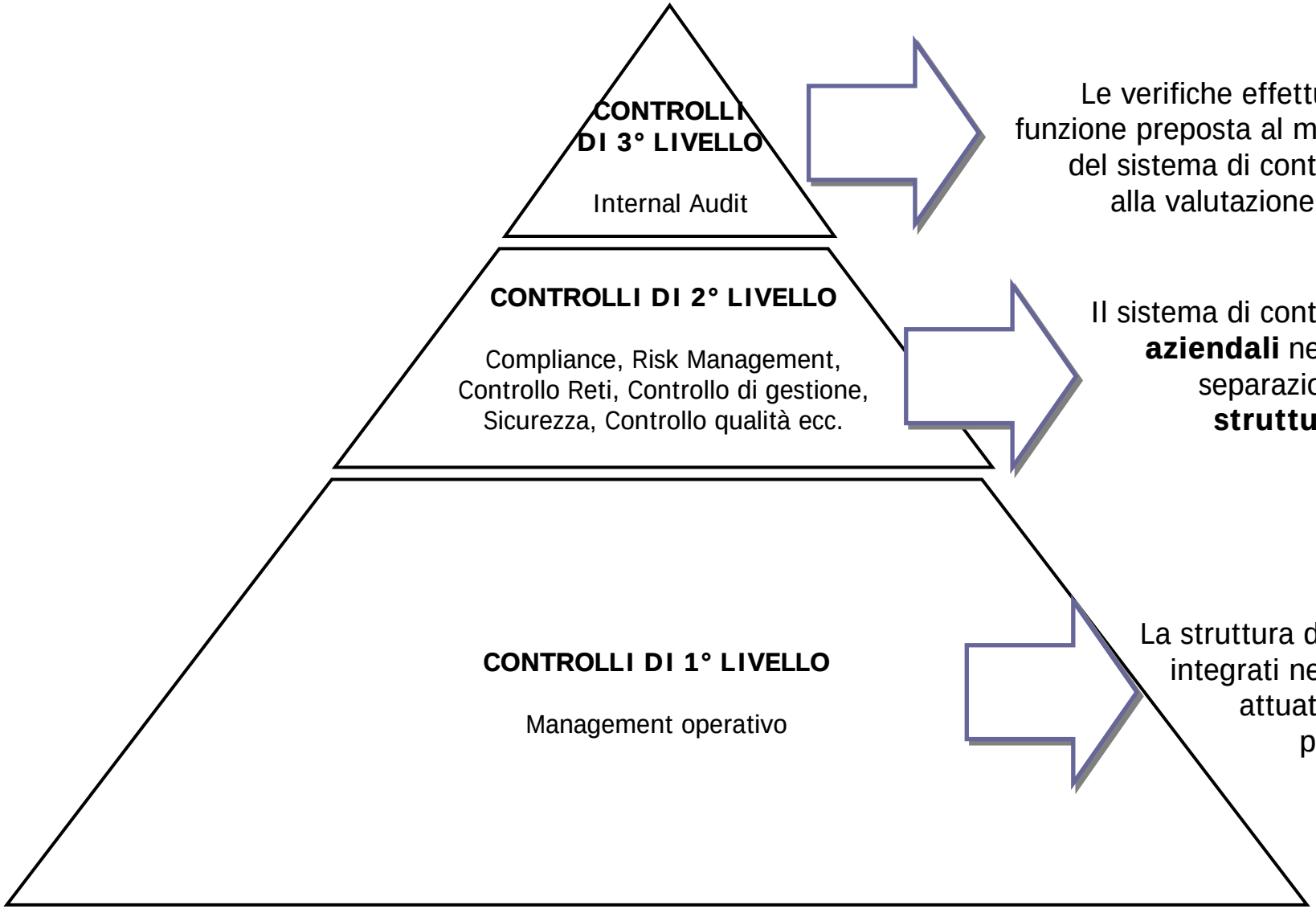
(…)

La funzione di revisione interna uniforma la propria attività agli standard professionali comunemente accettati a livello nazionale ed internazionale; in particolare verifica:

a) i processi gestionali e le procedure organizzative;
b) la regolarità e la funzionalità dei flussi informativi tra settori aziendali;
c) l'adeguatezza dei sistemi informativi e la loro affidabilità affinché non sia inficiata la qualità delle informazioni sulle quali il vertice aziendale basa le proprie decisioni;
d) la rispondenza dei processi amministrativo contabili a criteri di correttezza e di regolare tenuta della contabilità;
e) l'efficienza dei controlli svolti sulle attività cedute in outsourcing.

Principali attori del sistema dei controlli interni

La piramide dei controlli interni

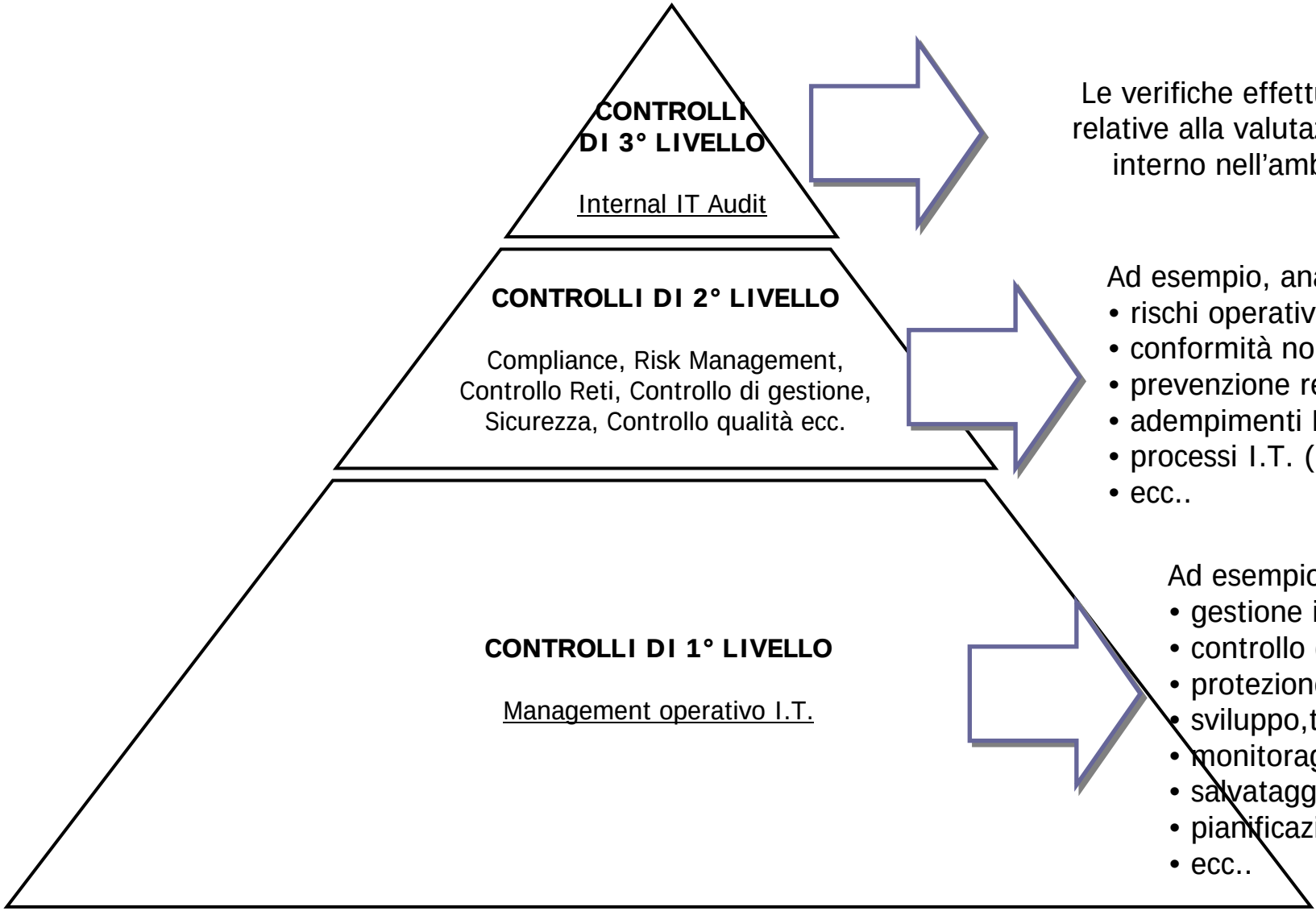


Le verifiche effettuate dall'**Internal Audit**, funzione preposta al monitoraggio del funzionamento del sistema di controllo nel suo complesso ed alla valutazione della sua adeguatezza

Il sistema di controlli svolti da **altre funzioni aziendali** nel rispetto del principio di separazione dei compiti e da **strutture specialistiche**

La struttura di controlli di linea, in larga parte integrati nei sistemi informatici aziendali, attuati da **tutti gli utenti** che partecipano ai diversi processi operativi

La piramide dei controlli interni nell'ambito dei sistemi informativi.



Le verifiche effettuate dall'**Internal IT Audit,** relative alla valutazione del sistema di controllo interno nell'ambito dei sistemi informativi.

Ad esempio, analisi e valutazione:
- rischi operativi I.T. (Risk Management);
- conformità normativa (Compliance);
- prevenzione reati informatici (OdV 231);
- adempimenti Dlgs.196 (Responsabile Privacy);
- processi I.T. (Dirigente Preposto);
- ecc..

Ad esempio, procedure/sistemi per:
- gestione iter autorizzativo di accesso;
- controllo dell'accesso logico ai dati;
- protezione fisica del CED;
- sviluppo,test e rilascio delle applicazioni;
- monitoraggio di performance e costi;
- salvataggi e D.R.;
- pianificazione/controllo delle attività;
- ecc..

Il ruolo della funzione di Audit alla luce del Regolamento ISVAP n. 20/2008

La funzione di Audit secondo il Regolamento ISVAP n. 20

MANDATO DELLA FUNZIONE DI AUDIT IN AMBITO ASSICURATIVO

(Regolamento ISVAP n. 20 del 26 marzo 2008)

Le imprese istituiscono una funzione di revisione interna, incaricata di monitorare e valutare l'efficacia e l'efficienza del sistema di controllo interno e le necessità di adeguamento, anche attraverso attività di supporto e di consulenza alle altre funzioni aziendali.

La funzione di Audit secondo il Regolamento ISVAP n. 20

POSIZIONE DELLA FUNZIONE DI AUDIT NELL'ORGANIZZAZIONE AZIENDALE

(Regolamento ISVAP n. 20 del 26 marzo 2008)

La **collocazione** della funzione nell'ambito della struttura organizzativa deve essere tale da **garantirne l'indipendenza e l'autonomia**, affinché non ne sia compromessa l'obiettività di giudizio.

La funzione di revisione interna **non dipende gerarchicamente** da alcun responsabile di aree operative.

Ai soggetti preposti alla funzione di revisione interna **non devono essere affidate responsabilità operative** o incarichi di verifica di attività per le quali abbiano avuto in precedenza autorità o responsabilità se non sia trascorso un ragionevole periodo di tempo.

La funzione **deve avere collegamenti organici** con tutti i centri titolari di funzioni di controllo interno.

La funzione di Audit secondo il Regolamento ISVAP n. 20

RESPONSABILE DELLA FUNZIONE DI AUDIT

(Regolamento ISVAP n. 20 del 26 marzo 2008)

Il responsabile della funzione è **nominato dall'organo amministrativo**.

Deve avere specifica **competenza e professionalità** per lo svolgimento dell'attività.

I **compiti** attribuiti al responsabile della funzione sono chiaramente **definiti ed approvati** con delibera del **Consiglio**, che ne fissa anche **poteri, responsabilità e modalità di reportistica** all' organo amministrativo stesso.

Il responsabile della funzione è dotato dell'**autorità** necessaria a garantire l'indipendenza della stessa.

La funzione di Audit secondo il Regolamento ISVAP n. 20

CARATTERISTICHE DELLA FUNZIONE DI AUDIT

(Regolamento ISVAP n. 20 del 26 marzo 2008)

La funzione deve essere **adeguata** in termini di **risorse umane e tecnologiche**.

Le risorse devono possedere **competenze specialistiche** e deve essere curato l'aggiornamento professionale.

Agli incaricati della funzione deve essere consentita **libertà di accesso** a tutte le strutture aziendali e alla documentazione relativa all'area aziendale oggetto di verifica.

La funzione di Audit secondo il Regolamento ISVAP n. 20

PIANIFICAZIONE DELLE ATTIVITA' DELLA FUNZIONE DI AUDIT

(Regolamento ISVAP n. 20 del 26 marzo 2008)

La funzione di revisione interna **pianifica** l'attività in modo da identificare le aree da sottoporre prioritariamente ad audit.

Il piano di audit è sottoposto all'**approvazione dell'organo amministrativo** e individua le attività a rischio, le operazioni e i sistemi da verificare, descrivendo i criteri sulla base dei quali questi sono stati selezionati e specificando le risorse necessarie all'esecuzione del piano.

Analogo procedimento è seguito in caso di variazioni significative ai piani approvati.

La funzione di Audit secondo il Regolamento ISVAP n. 20

REPORTING DELLE ATTIVITA' DELLA FUNZIONE DI AUDIT

(Regolamento ISVAP n. 20 del 26 marzo 2008)

La funzione **comunica** all'organo amministrativo, all'alta direzione ed all'organo di controllo la valutazione delle **risultanze** e le eventuali **disfunzioni e criticità**.

I rapporti di audit devono essere **obiettivi, chiari, concisi, tempestivi** e contenere suggerimenti per eliminare le carenze riscontrate e devono essere conservati presso la sede della società.

La revisione interna si conclude con l'attività di **follow-up**, consistente nella verifica a distanza di tempo dell'efficacia delle correzioni apportate al sistema.

La funzione di Audit nel gruppo Fondiaria-Sai

Il gruppo Fondiaria-Sai

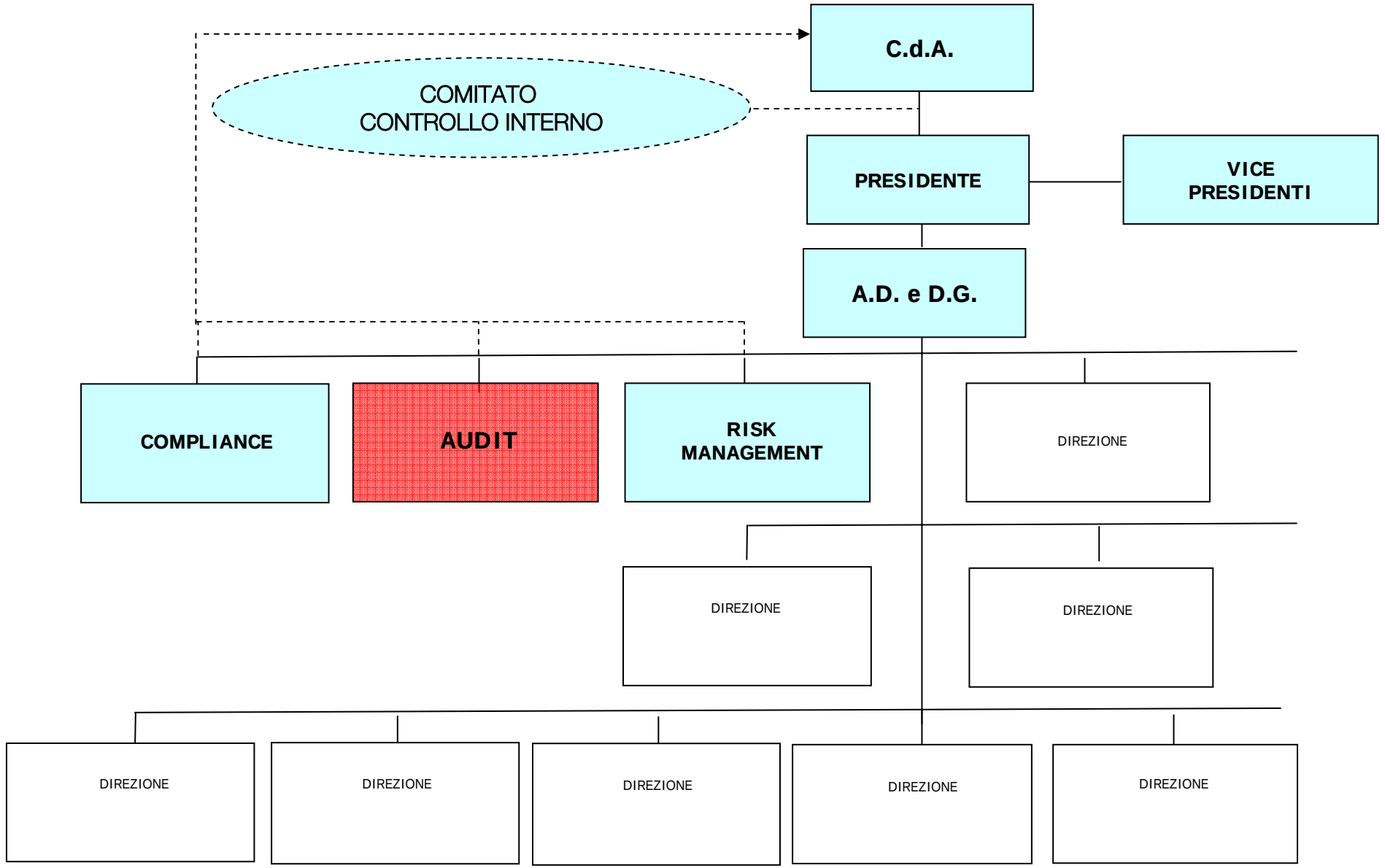
IL GRUPPO FONDIARIA-SAI: UNA VISIONE D'INSIEME

Alcuni riferimenti dimensionali al 31/12/2009:

RACCOLTA PREMI COMPLESSIVA: 12,307 miliardi	**RISERVE TECNICHE LORDE:** 31,718 miliardi	**SOCIETA' CONTROLLATE E COLLEGATE** ASSICURATIVE: 18 FINANZIARIE: 20 BANCARIE, SIM, SGR: 5 IMMOBILIARI E AGRICOLE: 54
TOTALE INVESTIMENTI: 34,216 miliardi	**NUMERO MEDIO DIPENDENTI:** 8.005	

Fonte: Bilancio consolidato 2009

Organigramma di Fondiaria-Sai



Fonte: Organigramma al 30/09/2010

N.B.: attualmente in fase di ridefinizione

IL COMITATO DI CONTROLLO INTERNO NEL GRUPPO FONDIARIA-SAI

La costituzione di un Comitato di Controllo Interno è prevista dal Codice di Autodisciplina delle Società Quotate alla Borsa Italiana che ne stabilisce anche la composizione (amministratori non esecutivi, la maggioranza dei quali indipendenti).

Nel gruppo Fondiaria-Sai sono stati costituiti dai rispettivi Consigli di Amministrazione due Comitati di Controllo Interno, relativamente alle due Compagnie quotate del Gruppo: Fondiaria-Sai e la controllata Milano Assicurazioni.

I principali compiti dei Comitati di Controllo Interno sono:

- assistere il Consiglio nella verifica periodica dell'adeguatezza e dell'effettivo funzionamento del sistema di controllo interno e, nell'ambito di tale sistema, anche dell'adeguatezza delle procedure amministrative e contabili;
- assistere il Consiglio nella identificazione e gestione dei principali rischi aziendali con una significativa possibilità di accadimento;
- vigilare sull'osservanza e sul periodico aggiornamento delle regole di corporate governance adottate dalla Compagnia e dalle proprie controllate;
- valutare il piano di lavoro della Funzione di Audit di Gruppo e ricevere le relazioni periodiche predisposte dalla stessa;
- esercitare, nell'ambito della gestione dei rapporti con i revisori esterni, una generale vigilanza sull'efficacia del processo di revisione contabile svolto dalla società di revisione.

Gli obiettivi della funzione di Audit nel gruppo Fondiaria-Sai

OBIETTIVI DELLA FUNZIONE DI AUDIT NEL GRUPPO FONDIARIA-SAI

(Manuale organizzativo gruppo Fondiaria-Sai)

Assistere gli **organi sociali** e il **Dirigente Preposto** nel costante monitoraggio del sistema dei controlli interni della Società.

Assistere il **Comitato di Controllo Interno** nello svolgimento operativo dei suoi compiti istituzionali.

Assistere l'**Organismo di Vigilanza** nell'espletamento dell'attività di vigilanza sull'osservanza del Modello di organizzazione, gestione e controllo e sull'efficacia ed adeguatezza dello stesso.

Gli obiettivi della funzione di Audit nel Gruppo Fondiaria-Sai

OBIETTIVI DELLA FUNZIONE DI AUDIT NEL GRUPPO FONDIARIA-SAI

(Manuale organizzativo gruppo Fondiaria-Sai)

Assicurare le attività di auditing al fine di valutare il **grado di adesione alle politiche** della Società da parte delle strutture organizzative aziendali.

Assicurare l'**individuazione delle aree di miglioramento** del sistema dei controlli interni della Società.

Garantire la **verifica** della corretta e puntuale realizzazione **delle azioni correttive** concordate.

Gli obiettivi della funzione di Audit nel gruppo Fondiaria-Sai

OBIETTIVI DELLA FUNZIONE DI AUDIT NEL GRUPPO FONDIARIA-SAI

(Manuale organizzativo gruppo Fondiaria-Sai)

Predisporre il piano annuale di Audit da sottoporre alla valutazione del Comitato di Controllo Interno e all'approvazione del Consiglio di Amministrazione della Società.

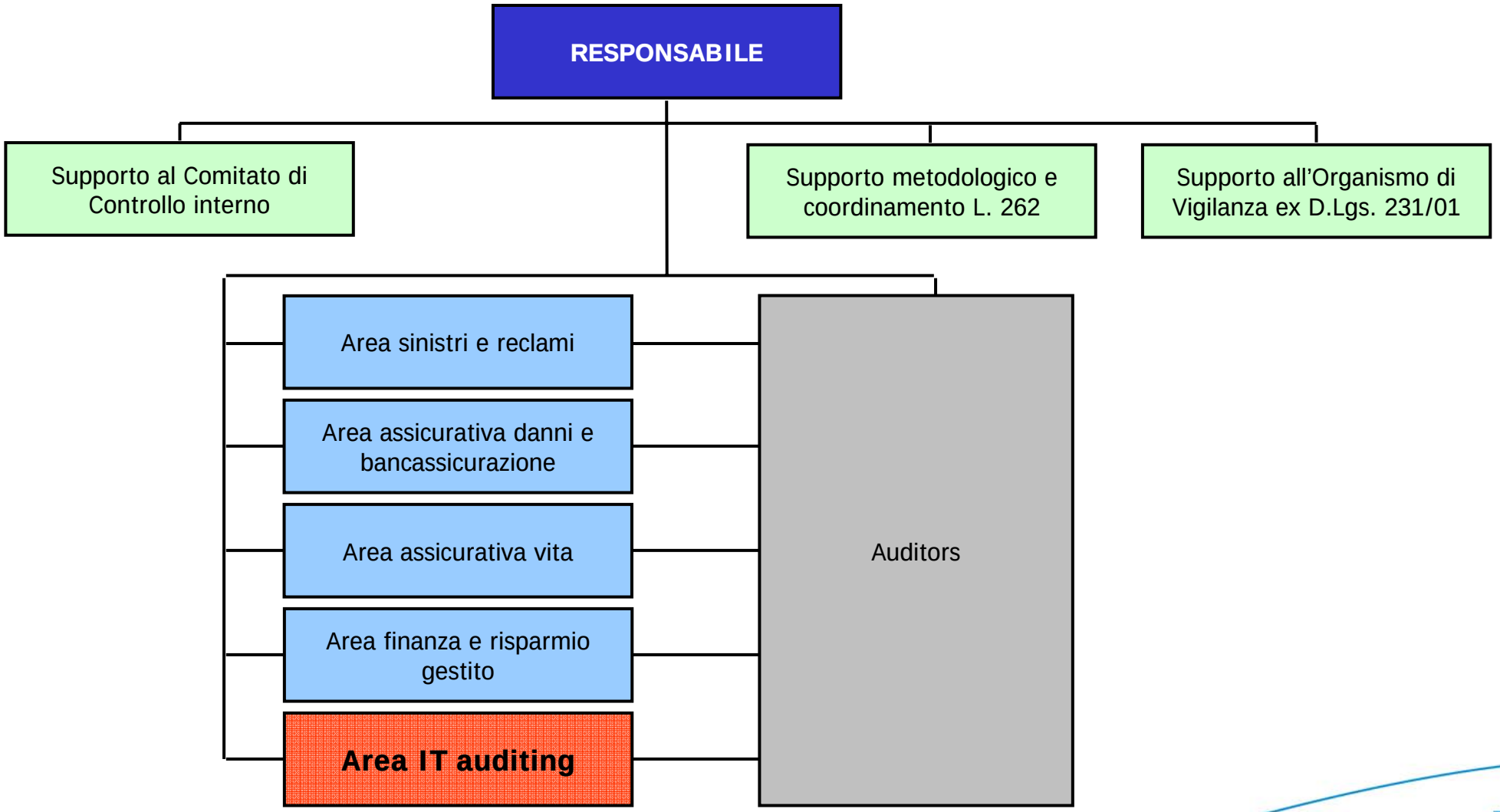
Garantire la **coerenza dei comportamenti operativi** delle strutture aziendali interne verso il "corpus normativo aziendale".

Assemblare, in collaborazione con Risk Management, **le evidenze** emerse dalla verifica del sistema dei controlli interni e di gestione dei rischi.

Gestire i **rapporti con le Società di revisione**.

La struttura della funzione di Audit del gruppo Fondiaria-Sai

ORGANIZZAZIONE DELLA FUNZIONE DI AUDIT NEL GRUPPO FONDIARIA-SAI



Un focus sull'IT audit

La struttura di IT Audit

COMPITI DELLE STRUTTURE INTERNE ALLA FUNZIONE DI AUDIT

(Manuale organizzativo del gruppo Fondiaria-Sai)

Area IT auditing

Controllo sull'adeguatezza, l'efficienza e l'efficacia dei sistemi informativi del Gruppo. In particolare, i principali obiettivi sono:

• la valutazione e il monitoraggio del sistema informatico, con particolare riguardo ai seguenti aspetti:

1) sicurezza fisica;
2) sicurezza logica;
3) affidabilità delle procedure;
4) qualità del servizio reso in relazione alle esigenze concrete degli enti utilizzatori del servizio;

• supporto alle funzioni aziendali nell'attività di re-engineering delle procedure informatiche;

• supporto informatico alle attività di revisione;

• analisi dei processi al fine della copertura dai rischi tecnologici.

La struttura di IT Audit

L'EVOLUZIONE DELL'ATTIVITA' DI IT AUDIT

Nel gruppo Fondiaria-Sai, l'IT auditing ha avuto una progressiva evoluzione nel corso dell'ultimo decennio a fronte della maggiore complessità dei compiti assegnati alla struttura, che trae origine principalmente:

- dall'esigenza di conformarsi alle previsioni della normativa, soprattutto di settore;
- dalle numerose variazioni intervenute negli assetti societari del Gruppo (una su tutte, la fusione per incorporazione di "La Fondiaria Assicurazioni" in "Sai – Società Assicuratrice Industriale");
- dalla rapida e continua trasformazione e diversificazione della tecnologia;
- dalle esternalizzazioni avviate in ambito IT (principalmente, la joint venture con Hp-EDS per la gestione dell'infrastruttura informatica).

In tale contesto, negli ultimi dieci anni l'attività di IT audit ha assunto all'interno del Gruppo una maggiore rilevanza, passando dall'essere principalmente un supporto informatico alle attività di revisione interna ed esterna (p.e. certificazione di bilancio) ad una struttura dotata di compiti e responsabilità delineati, nella quale operano addetti provvisti di professionalità e competenze specifiche.

All'interno della funzione di Audit di Gruppo, la struttura di IT Audit è attualmente costituita da 2 risorse, entrambe dotate di certificazione CISA.

La pianificazione dell'attività di IT audit

La pianificazione delle attività di audit

PIANIFICAZIONE DELLE ATTIVITA' DELLA FUNZIONE DI AUDIT

Predisposizione del piano

La **funzione di Audit** predispone per Fondiaria-Sai e per le società del Gruppo un Piano annuale delle attività (Piano di Audit). La formulazione del Piano di Audit avviene in base ad una serie di elementi che determinano una scala di priorità delle attività da sottoporre ad audit, utilizzando anche le informazioni prodotte dalla struttura di Risk Management e tenendo conto delle eventuali problematiche di rilievo che emergano nell'ambito dell'attività del Comitato di Compliance e di Coordinamento Funzioni di Governance.

Valutazione del piano

Il Piano di Audit viene valutato dal **Comitato di Controllo Interno.** Tale Piano, in considerazione della presenza di numerosi processi di Gruppo, tiene conto delle sinergie ottenibili dallo svolgimento di analisi accentrate, provvedendo comunque a identificare le peculiarità delle singole società che vengono riflesse nelle attività inserite nel Piano di ciascuna di esse.

Approvazione del piano

Il Piano di Audit viene sottoposto all'approvazione del **Consiglio di Amministrazione** di ciascuna società del Gruppo.

La pianificazione delle attività di IT audit

IL PIANO DI IT AUDIT

Il piano delle attività di IT audit è una componente del Piano di Audit annuale predisposto dalla Funzione per ciascuna delle società del Gruppo. L'identificazione delle aree da sottoporre a verifica viene svolta tenendo conto, in primo luogo, dei seguenti elementi:

- gli avanzamenti del piano strategico sulla tecnologia dell'informazione e comunicazione (ICT) con le relative variazioni ed evoluzioni inerenti i sistemi e le applicazioni di business;
- le risultanze delle analisi dei rischi IT effettuate dalla funzione di Risk Management;
- richieste di intervento provenienti dal board oppure dagli altri attori del sistema di controllo interno (p.e. Collegio Sindacale, Dirigente Preposto, Comitato di Controllo Interno, ecc.)
- richieste di intervento provenienti dai management operativo, anche non appartenente all'I.T.;
- specificità, per quanto riguarda sistemi/applicazioni, di alcune società del Gruppo;
- fatti rilevanti emersi nel corso dell'anno (p.e. fusioni societarie, tentativi di truffa, reengineering di processi di business, ecc..) ;
- considerevole impatto, in termini operativi ed economici, del contratto di outsourcing in vigore con Hp-EDS (ed attuato attraverso la società Fondiaria-Sai Servizi Tecnologici);
- entrata in vigore di eventuali novità normative/legislative, con effetti sui sistemi informativi (p.e. Amministratori di sistema);
- programmazione di attività di follow-up.

La funzione di Audit: il reporting

REPORTING DELLE ATTIVITA' DELLA FUNZIONE DI AUDIT

A conclusione di ciascuna attività svolta, il responsabile della funzione di Audit riferisce in merito alle risultanze emerse nel corso degli interventi effettuati, attraverso la **trasmissione dei Rapporti di Audit**:

- all'**Amministratore Delegato** della Capogruppo;
- all'**Alta Direzione** delle società del Gruppo eventualmente interessate dall'ambito di operatività;
- ai **responsabili dei processi** analizzati.

Con riferimento alle **società quotate**, le risultanze delle attività di audit svolte vengono presentate su base, di norma trimestrale, ai Comitati di Controllo interno per le aree di pertinenza e riepilogate semestralmente da questi ultimi in una relazione presentata ai rispettivi Consigli di Amministrazione.

Con riferimento alle **altre compagnie del Gruppo**, le risultanze delle attività di audit svolte vengono riepilogate in una relazione annuale presentata al Consiglio di Amministrazione in concomitanza con la presentazione del Piano annuale.

Le principali problematiche nello svolgimento delle attività

Le principali problematiche dell'attività di audit

Di seguito, vengono evidenziate alcune delle principali problematiche relative allo svolgimento dell'attività di audit e di IT audit nel gruppo Fondiaria-Sai:

- risulta talvolta difficoltoso rendere comprensibili ai soggetti destinatari, solitamente non dotati di competenze specifiche, le risultanze sintetiche delle attività di IT audit, connotate in molti casi da un elevato contenuto tecnico;
- la molteplicità di società, ambiti, sistemi ed applicazioni oltre che di nuove priorità che emergono nel corso dell'attività spesso non consentono di adottare, nella pianificazione degli incarichi di audit, un ulteriore importante criterio fondato sul principio di ciclicità (rotazione) di intervento sulle diverse aree;
- la piena integrazione tra i compiti delle funzioni di controllo (p.e. Audit, Risk Management, Compliance, ecc) risulta in alcuni casi difficoltosa, poiché non è sempre identificabile con certezza il confine delle competenze di ognuna di esse, confine che talvolta risulta essere solamente di tipo teorico. Il rischio di interferenza nelle competenze altrui o di mancanza di "copertura" di alcune aree di rischio, nel gruppo Fondiaria-Sai risulta mitigato dalla costituzione del "Comitato di Compliance e di Coordinamento Funzioni di Governance";
- talvolta non risulta facile l'individuazione del rischio di frode nei processi aziendali e nei sistemi informatici che supportano tali processi.

Grazie

Luca Martoglio
Fondiaria-Sai S.p.A.
AUDIT
luca.martoglio@fondiaria-sai.it